**IN THE UNITED STATES DISTRICT COURT**
**FOR THE WESTERN DISTRICT OF PENNSYLVANIA**

| | |
|---|---|
| ASHLEY POPA, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>HARRIET CARTER GIFTS, INC., a Pennsylvania corporation, and NAVISTONE, INC., a Delaware corporation,<br><br>Defendants. | **Case No. 2:19-cv-00450-WSS** |

**PLAINTIFF'S OPPOSITION TO**
**DEFENDANTS' SECOND MOTION FOR SUMMARY JUDGMENT**

**TABLE OF CONTENTS**

## TABLE OF AUTHORITIES

**Cases** **Pages**

**Statutes**



**Rules**



**Other Authorities**

## INTRODUCTION

Plaintiff Ashley Popa brought this class action to protect her online privacy after discovering that Harriet Carter Gifts, Inc. ("Harriet Carter") and NaviStone, Inc. ("NaviStone") had intentionally wiretapped her and other Internet users' communications with the Harriet Carter website, in order to track, de-anonymize, and market to them. By deploying code created by NaviStone, which Harriet Carter intentionally installed on its website, users' communications with HarrietCarter.com were surreptitiously intercepted by NaviStone. Those communications are then used by NaviStone to trace back users' digital presence until their physical presence can be found, identified, and marketed to—including by mailing users Harriet Carter catalogs.

In its prior opinion in this case, the Third Circuit held that these actions ran afoul of the Pennsylvania Wiretapping and Electronic Surveillance Control Act ("WESCA")—unless Defendants could show that Plaintiff and other web users somehow consented to the interception of their communications. The facts developed in discovery establish that consent to this wiretap did not occur and was not possible, despite Defendants' claims to the contrary. Plaintiff was never asked to explicitly and affirmatively consent to an interception of her data by a third party, whose role on the site had nothing to do with the site's functionality. Plaintiff, like most Internet users, had no idea that this type of code could be running in the background of a retailer's website. And Harriet Carter's privacy policy—which was hidden behind a link in the footer of its website and was accessed by less than 1% of website visitors—failed to sufficiently disclose the data tracking practices that were surreptitiously occurring when users visited the website. Moreover, even if the privacy policy *did* accurately disclose that information, obtaining the requisite *prior* consent was virtually impossible because NaviStone's software began collecting users' communications the instant they arrived on Harriet Carter's website, and before there was time to navigate to and/or read the privacy policy.

Plaintiff and other Internet users simply could not have given their prior consent to NaviStone's wiretap of their communications. Plaintiff therefore has sufficient evidence to take her WESCA claim to trial, and the Court should deny Defendants' Second Motion for Summary Judgment ("Motion").

## FACTUAL BACKGROUND

Much of the factual background underlying this case was set forth in Plaintiff's previous opposition to Defendants' first motion for summary judgment. *See* ECF 98. For the sake of the Court, however, Plaintiff summarizes the most relevant facts here, as well as additional evidence gathered since this matter was remanded from the Third Circuit.

### A. Harriet Carter and NaviStone Wiretap Harriet Carter's Website Visitors.

In or around August 2016, at the urging of NaviStone, Harriet Carter procured NaviStone's services to collect users' electronic communications with Harriet Carter's website (the "Website"), and to use the information to deanonymize the website visitors and send them catalog mailings. CSOMF ¶¶ 116, 178.[1] To effectuate this, NaviStone provided Harriet Carter with a line of JavaScript code (the "Code" or "OneTag"), which Harriet Carter added to each page of its website. CSOMF ¶ 27. The operation and functionality of Harriet Carter's website did not rely in any way on the use of the Code. CSOMF ¶ 186. But once its Code was installed, NaviStone had "an open door" to Harriet Carter's website. CSOMF ¶ 12. The Code would deploy instantly when a website user arrived to the Harriet Carter website, CSOMF ¶ 384, but

[1] Citations to "CSOMF" refer to Plaintiff's Response to Defendants' Concise Statement of Material Facts in Support of Motion for Summary Judgment (¶¶ 1–175) and Plaintiff's Concise Statement of Other Material Facts (¶¶ 176–259), ECF 99, the continuation to which—Plaintiff's Response to Defendants' Concise Statement of Material Facts in Support of Defendants' Second Motion for Summary Judgment (¶¶ 260–380) and Plaintiff's Statement of Other Material Facts (¶¶ 381–489)—is submitted contemporaneously with Plaintiff's Opposition.

was not visible to a Website user without using web developer tools to determine that the code is there and then figures out how to decipher the code. CSOMF ¶ 155.

While running in the background of the Website visitor's device, OneTag "listens in" to the visitor's Website communications with Harriet Carter. The Code builds what is called a "payload" of information. CSOMF ¶ 198. Each payload includes the users' IP address and pseudonymous cookie identifiers,[2] but also includes information on the user's communications with the Website including the referrer URL (or the URL of the page from which the user navigated to the current page), the URL, the Page Title of the webpage, and any URL query string of the page the user requested and/or navigated to. CSOMF ¶¶ 198, 227–28.[3] The NaviStone Code also captured: when a user added an item to their cart, the product(s) added to their cart (including the quantity), the price(s) of the product(s) added to the cart, the cart total (including shipping and tax charges), whether a user filled out a form field, and whether a user input their e-mail address into any field.[4] CSOMF ¶¶ 43–44. The information collected by

[2] NaviStone ultimately uses these identifiers, in conjunction with other third-parties, to obtain personally identifying information (names and addresses) of website users to send them catalogs by mail. CSOMF ¶ 244–46.

[3] For Harriet Carter, the URL and URL query strings provided significant details on the search request or page viewed. *Id.* For example, each product page identified the product within the URL. *Id.* Product information was, likewise, included in the Page Title. CSOMF ¶ 476. This interception alone gave NaviStone details on what products a user viewed and what path they took to arrive at that product page. CSOMF ¶ 41.

[4] Prior to June 20, 2017, NaviStone collected the actual information a HarrietCarter.com user entered into various form fields, including but not limited to name, address, email address, phone numbers, etc. CSOMF ¶¶ 57, 229–30. After June 20, 2017, when the Gizmodo article discussed in Plaintiff's Complaint was published, NaviStone edited the OneTag Code—unbeknownst to Harriet Carter—in order to stop collecting the information entered into those form fields, but still monitored and recorded every time a form field was filled it. CSOMF ¶¶ 56–57.

NaviStone's OneTag went beyond what third-party software normally collects from website visitors. CSOMF ¶ 476.

**B. Defendants' Collection of Plaintiff's Communications.**

In early 2018, while at her home in Pennsylvania, Ms. Popa visited Harriet Carter's Website using the Safari browser on her iPhone. CSOMF ¶¶ 124–25, 461–63. While on the Website, a pop-up appeared, and Ms. Popa entered her e-mail address into the form and believes she submitted it. *Id.* She knows at minimum she searched for pet stairs and recalls adding the pet stairs to her cart and filling out form field information at the check-out. *Id.*

From the moment Plaintiff arrived on the Harriet Carter website, NaviStone's OneTag would have deployed immediately to intercept her communications with Harriet Carter. *See* CSOMF ¶¶ 263, 351–52. Specifically, NaviStone's OneTag would have collected data showing, at minimum: that Plaintiff told Harriet Carter her email address; that Plaintiff specifically searched the Harriet Carter website for pet stairs; that she viewed pet stairs; the specific pet stairs she placed in her cart; the price of those pet stairs; and information on any other products that Plaintiff browsed during her visit. CSOMF ¶ 125.[5]

Ms. Popa does not recall seeing a link to a privacy statement on Harriet Carter's website or reading any privacy policy. CSOMF ¶ 176.[6] She had no idea that NaviStone's OneTag Code

[5] Defendants assert in their brief that Plaintiff has "no evidence" of her visit, but Plaintiff's deposition testimony regarding her visit to the Harriet Carter website *is* admissible evidence. *See* Fed. R. Civ. P. 56(c)(1)(A). Moreover, though Defendants are correct that Plaintiff does not have a record of her visit(s) to the website, that is because her browsing history and cookies were deleted before she was ever aware that she had been wiretapped by Defendants. CSOMF ¶ 464. This fact should not diminish the veracity or weight of her deposition testimony.

[6] When websites have pop-up or other mechanism to show visitors their privacy policies immediately upon arrival to the website, Ms. Popa will skim those privacy policies because she doesn't have to go searching for it. CSOMF ¶ 345. But here, Harriet Carter never alerted Plaintiff to the existence of the website's Privacy Statement during her visit to the Website. CSOMF ¶ 176.

was running on her browser or that her communications were being intercepted by NaviStone. CSOMF ¶ 465.[7] Despite having a nursing degree, Ms. Popa has no idea how to determine whether code, such as NaviStone's, is operating on any website she visits. CSOMF ¶¶ 471, 476. Plaintiff believes she should have been informed if she was communicating with any other source other than Harriet Carter and that her communications with Harriet Carter on its website should not have been shared with NaviStone without her consent. CSOMF ¶ 477.

**C. The Harriet Carter "Privacy Statement."**

The link to the Privacy Statement on Harriet Carter's website was located all the way at the bottom of the web page, below the display of products sold by Harriet Carter. CSOMF ¶ 422. Despite the technology being available, Harriet Carter did not have a pop-up or banner alerting users to its Privacy Statement during the relevant time period, and never considered instituting a pop-up or banner. CSOMF ¶¶ 432–33. Harriet Carter did not require website visitors to read or accept the Privacy Statement during the relevant time period, and never considered instituting either requirement for visitors. CSOMF ¶ 425. During the relevant time period for this case, less than 1% of users to the Harriet Carter website ever accessed the website's privacy policy page during the relevant time period. CSOMF ¶ 427. It is not known how many of that fraction of a percent of visitors that viewed the policy actually read it.

For the less than 1% of visitors who even viewed the Privacy Statement, various design choices, and the structure and language of the policy itself, prevented users from fully comprehending the type of third-party data collection that Harriet Carter allowed to occur on their website. Just by having a document entitled "Privacy Statement," visitors to

[7] Had Plaintiff known that OneTag was running, she may never have used the Harriet Carter website in the first place; since discovering the interception that occurred during her visit, she is now too concerned about her data being secretly collected to return to the Harriet Carter website. CSOMF ¶ 464.

harrietcarter.com would likely assume and misinterpret that Harriet Carter promised to protect their privacy. CSOMF ¶ 428. Further contributing to this assumption, the policy started with assurances that Harriet Carter "believe[s] you have a right to a safe, secure online shopping experience. We are committed to both protecting your privacy." CSOMF ¶ 429. Similarly, later provisions in the Privacy Statement profess that Harriet Carter "adopts an 'opt-in' mentality to all promotional information," including customer lists, promotional emails, and catalog mailings—even though NaviStone's software was collecting users' data without their knowledge or consent *specifically to de-anonymize them and send them catalog mailings*. CSOMF ¶ 430.[8]

Indeed, for the rare Harriet Carter website visitor that actually navigated to the policy, if they actually read the entire Privacy Statement, it fails to sufficiently describe NaviStone's technology and its wiretapping functions. CSOMF ¶¶ 436-437.

The very first section of the Privacy Statement is titled "When I visit Harrietcarter.com, what information is gathered about me and why?" CSOMF ¶ 432. It seems only natural that, if a web visitor wanted to know what information was gathered about them and why, that this is where a reasonable person would look for that. Yet, there is no information about NaviStone's wiretap in that section. Instead, what little information exists that alludes to NaviStone's activity is included several subheadings down under the "Who Else Has Access to the Information I Provide to HarrietCarter.com?" section, and buried under a subheading titled "Third Party." CSOMF ¶ 433. But even this section is not straightforward, beginning with a discussion about visitors who buy gifts for their friends, and a promise that "HarrietCarter.com does not sell, rent,

[8] The Privacy Statement contains no provision describing how to opt-out of Harriet Carter or third parties collecting, using, and sharing their data. CSOMF ¶ 323. Indeed, common methods that a user themselves might employ to try to prevent data collection—such as disabling third-party cookies—will not prevent NaviStone's OneTag from intercepting their communications. CSOMF ¶¶ 61, 63.

or give away your personal information to anyone." CSOMF ¶ 434. Only at the very bottom of this section does the policy reveal that Harriet Carter "may from time to time contract with third party vendors to serve ads . . . or to send our catalogs to customers." CSOMF ¶ 435. This generic reference to online ads and catalog mailings, however, provides no clear explanation of who the vendors are, how they are getting the user's data, or what that data consists of. CSOMF ¶ 437. And there is no mention of NaviStone's name anywhere in the policy. Privacy Statement; CSOMF ¶ 328.

Additionally, just as with any webpage on the website, the OneTag Code would deploy immediately and start collecting data about a website visitor when they visited the Privacy Statement, before they could even read it. CSOMF ¶¶ 263, 326–27, 351.

**D. Consent and Online Privacy.**

As evinced by the fraction-of-a-percent of visitors that actually navigated to the Harriet Carter Privacy Statement, privacy policies are frequently missed or ignored by typical website visitors. CSOMF ¶ 277; Stipulation of Fact.[9] This is, in part, because users can easily miss a website's privacy policy when it is buried in a link at the bottom of a website. CSOMF ¶ 278.

Privacy policies' content, even if website visitors manage to navigate to the policies, are also generally insufficient to get meaningful consent from users as to the practices described therein. Privacy policies, for example, are generally long, and this length makes it particularly difficult for website visitors to fully comprehend their contents; one study found that it would take the average Internet user nearly 244 hours per year to read the privacy policies of the

[9] Discussion of typical Internet users' and online consumer behavior in this sub-section, which is based on the expert report and testimony of Plaintiff's expert Dr. Ari Waldman, a professor of law and sociology, is rooted in statistical literature that objectively reviewed the reasonableness of certain practices given evidence about "what the typical user can and cannot do." CSOMF ¶ 307.

websites they visit just once. CSOMF ¶ 284. Privacy policies are also written by lawyers and for lawyers, and written in vague and opaque language. CSOMF ¶¶ 279, 283. This vague and confusing language prevents many individuals from understanding what information is actually being collected from them when they visit a website. CSOMF ¶ 281. Harriet Carter's Privacy Statement is no different.

Indeed, web designers can also use so-called "dark patterns"—interface design choices that benefit an online service by coercing, steering, or deceiving users into making certain decisions that a user otherwise might not make—in the presentation of a privacy policy in order to hide, deceive, and goad users into disclosure. CSOMF ¶ 287. For example, rather than recognizing privacy policies as statements of corporate data collection and use practices, many nonexperts are deceived into thinking that having a privacy policy means a company is promising to protect users' privacy. CSOMF ¶ 288. In one study of individuals' knowledge about online privacy and data tracking, over eighty percent of the individuals involved earned "D" or "F" grades. CSOMF ¶ 292. Even experts find privacy policies misleading, with one study finding that various privacy scholars and experts came to very different understandings of the language in a single privacy policy. CSOMF ¶ 289.

Because online users generally cannot comprehend how the aggregation of seemingly innocuous data can undermine their privacy and security, individual consumers' online decision-making regarding their privacy does not generally reflect "their full understanding of what it is they are consenting to." CSOMF ¶¶ 290-91. Indeed, to give consent to a website's collection of their data, users "have to be in a position to appreciate [the] risks" that come from using a website, but "a lot of times those risks are hidden from people, or they are not accessible, given the cognitive limitations that we do know that companies rely on when providing information to

consumers." CSOMF ¶ 282. Privacy policies are also often presented to individuals as take-it-or-leave it statements of corporate practices, essentially like a "browsewrap" agreement, thus depriving website visitors of any real, meaningful choice regarding their privacy. CSOMF ¶ 280. As a result, online users' privacy choices often should be given very little weight, because privacy policy design often favors the interests of the company over its users, and the best that any one user can do is manage their privacy haphazardly. CSOMF ¶ 286. Indeed, the notion that online consumers can consent to the collection of their data under the described privacy policy regime is considered by some experts to be a myth. CSOMF ¶ 294.

Various tools exist, however, that websites can use in order to get Internet users' consent to their data collection practices, including allowing third parties to collect users' information. CSOMF ¶ 295. Alternative ways of alerting users to the existence of a privacy policy, such as cookie banners and pop-ups, have become much more commonplace. Clayton Dep., 93:8-15. CSOMF ¶¶ 297-98. Other strategies also exist to alert users to privacy policies and the collection of users' data, such as visceral notices using sound, color, or audio alerts. CSOMF ¶ 299. Various strategies also exist to make privacy policies themselves significantly more readable and understandable to the average Internet user, such as creating a "tiered" privacy policy that summarizes a policy's contents at a high level and highlights the most critical information contained in the policy. CSOMF ¶ 295.

## LEGAL STANDARD

To prevail on a motion for summary judgment, a movant bears the initial burden of showing that there are no genuine issues of material fact in dispute, and they are entitled to judgment as a matter of law. *Hartford Steam Boiler Inspection v. Int'l Glass Products, LLC*, No. 2:08-cv-1564, 2016 WL 5468111, *10 (W.D. Pa. Sept. 29, 2016). If they have met that burden, the non-movant must then point to some affirmative piece of evidence that creates a genuine

dispute for trial. *Williams v. Borough of W. Chester, Pa*., 891 F.2d 458, 460 (3d Cir. 1989). Where the non-movant has demonstrated a genuine dispute about a material fact whereby a reasonable jury could return a verdict for the non-moving party, summary judgment is unwarranted. *Anderson v. Liberty Lobby, Inc*., 477 U.S. 242, 247 (1986). In deciding a summary judgment motion, a court views the facts in the light most favorable to the nonmoving party and must draw all reasonable inferences, and resolve all doubts, in favor of the nonmoving party. *Matreale v. N.J. Dep't of Mil. & Veterans Affairs*, 487 F.3d 150, 152 (3d Cir. 2007).

## ARGUMENT

The Third Circuit directed this Court, on remand, to address: (1) "where Popa's browser accessed the Harriet Carter website," and (2) "whether Harriet Carter posted a privacy policy and, if so, whether that policy sufficiently alerted Popa that her communications were being sent to a third-party company." *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 131 (3d Cir. 2022).

Defendants no longer challenge the location of the interception in light of the Third Circuit's holding. *See* MSJ, generally. Indeed, Ms. Popa was in Pennsylvania when she accessed the Harriet Carter website. CSOMF ¶ 452.

The only issue now remaining in Defendants' second summary judgment motion is whether Ms. Popa consented to NaviStone's interception of her communications with Harriet Carter. As the party seeking the benefit of WESCA's all-party consent exception, Defendants bear the burden to prove that "*all parties* to the communication have given *prior* consent to the interception." 18 Pa. C.S. § 5704(4); *see In re Pharmatrak, Inc.*, 329 F.3d 9, 19 (1st Cir. 2003); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1028 (N.D. Cal. 2014). The consent "standard is one of a reasonable person," and is an objective—not subjective—standard. *Com. v. Byrd*, 235 A.3d 311, 319 (Pa. 2020). Consent can be express or implied, but to be implied it must be actual, not constructive consent. *In re Pharmatrak, Inc.*, 329 F.3d at 19. For implied consent Defendants

must demonstrate "the person being recorded knew or should have known that the conversation was being recorded." *Popa*, 52 F.4th at 132 (internal quotation marks and citation omitted). Consent may not be casually inferred, and Defendants' proof must be compelling. *In re Pharmatrak, Inc.*, 329 F.3d at 20 (citing *Griggs-Ryan v. Smith*, 904 F.2d 112, 117 (1st Cir. 1990)). As is explained in detail below, Defendants failed to meet their burden to show that there are no genuine disputes of material fact and that Plaintiff consented to Defendants' wiretap as a matter of law.

Additionally, Defendants ask this Court to hold WESCA unconstitutional under the First and Fourteenth Amendments. These arguments misapply constitutional law and seek to resurrect their argument that an adverse ruling in this case will lead to a "parade of horribles," an argument the Third Circuit already rejected on appeal.

## I. Plaintiff Did Not Consent to the Interception of Her Communications by Either Harriet Carter or NaviStone.

### A. As the Third Circuit has made clear, a sender of electronic communications does *not* automatically consent to the interception of their communications by a direct recipient under WESCA.

Defendants ask this court to find that a direct recipient of a communication cannot be held liable under WESCA, suggesting that the Third Circuit's prior decision in this case only held that a direct recipient might *intercept* a communication under WESCA, but cannot be held *liable* under WESCA. MSJ at 10. Specifically, Defendants claim that although the interception may have occurred, Pennsylvania law allegedly provides that a sender of a communication consents as a matter of law to its "interception" by the intended recipient. *Id.*

This issue was expressly foreclosed by the Third Circuit's prior decision in this case. *Popa v. Harriet Carter Gifts, Inc.,* 52 F.4th 121, 129 (3d Cir. 2022) ("This reframing, when paired with our analysis of the WESCA's plain language and statutory history, persuades us the

Pennsylvania Supreme Court would rule that there is no sweeping direct-party exception to civil liability under the WESCA."). The Third Circuit's opinion emphatically rejected Defendants' argument that WESCA still retains a direct-party exception—which would allow a party to a communication to lawfully intercept it without the other person's consent—stating that such a rule would make the all-party consent requirement of WESCA "disappear." *Popa*, 52 F.4th at 128. Defendants now ask this Court to re-write WESCA and read a direct party exception into the consent provision, but it cannot do so. The Third Circuit's holding was not a theoretical question separate from issues of liability, and the Circuit concluded its reasoning by emphasizing that "NaviStone and Harriet Carter cannot avoid liability [under WESCA] merely by showing that Plaintiff communicated directly with NaviStone's servers." *Id.* Indeed, the Circuit's opinion explicitly rejected Defendants' citations to *Commonwealth v. Diego*, 119 A.3d 370 (Pa. Super. Ct. 2015), which they again rely upon to in their Motion. *See Popa,* 52 F.4th at 129 ("We therefore discern no principled basis to rule that *Diego* authorizes, absent consent, the kind of surreptitious tracking that occurred here.").

If the Third Circuit had been convinced that *Diego* and other Pennsylvania cases cited by Defendants held that consent *as a matter of law* exists for intended recipients, it could have said so. Instead, the Circuit held that both NaviStone and Harriet Carter can be held liable for the surreptitious interception of Plaintiff's communications with them, even if NaviStone was a direct party, and remanded the case to determine whether Defendants could prove that Plaintiff had actual or constructive knowledge of the interception such that she consented to it. *See Popa*, 52 F.4th at 132-33. This is a question of fact, not something easily disposed of as a matter of law. Plaintiff has an array of evidence to demonstrate that she did not consent to Defendants'

interception of her communications, which at the very least creates a genuine dispute regarding that fact, as discussed above and *infra* in Part II.

### B. Defendants' claim that NaviStone operated as Harriet Carter's agent does not excuse NaviStone eavesdropping on Plaintiff's communications with Harriet Carter without Plaintiff's consent.

The Court should also reject Defendants' claim that Plaintiff consented to NaviStone's interception of her communications because NaviStone was simply acting as Harriet Carter's agent at the time, such that the two entities should be treated as "one and the same."

Preliminarily, this argument is an affirmative defense that procedurally cannot be raised for the first time this late in the case. *See* Fed. R. Civ. P. 8(c); *Robinson v. Johnson,* 313 F.3d 128, 134–35 (3d Cir. 2002) ("The purpose of requiring the defendant to plead available affirmative defenses in his answer is to avoid surprise and undue prejudice by providing the plaintiff with notice and the opportunity to demonstrate why the affirmative defense should not succeed."); *Ingraham v. United States,* 808 F.2d 1075, 1079 (5th Cir. 1987) ("Central to requiring the pleading of affirmative defenses is the prevention of unfair surprise. A defendant should not be permitted to 'lie behind a log' and ambush a plaintiff with an unexpected defense."). Here, Defendants failed to raise their agency defense in their answer, failed to raise the agency defense in their first motion for summary judgment, and now—for the first time—are raising the argument in their second motion for summary judgment, well after Plaintiff had an opportunity to cross-examine Defendants' witnesses on the subject to build a record around why NaviStone was not Harriet Carter's agent merely because it was a vendor.

But even assuming Defendants can raise this argument,[10] a third-party software vendor, like NaviStone is simply not an intended recipient of communications between a website visitor and a website like Harriet Carter's, even if they directly "listen" to the communications when their code intercepts the communications in real-time. *See Commonwealth v. Murray*, 223 A.2d 102, 108–09 (Pa. 1966) (holding that wiretap occurred where third party intercepted telephone communication in real-time with assistance of one participant in phone call); *see also Popa*, 52 F.4th at 132 (discussing whether Harriet Carter had "sufficiently alerted Popa that her communications were being sent to a third-party company"). As another court explained when ruling on a similar case involving NaviStone's code:

> [I]t cannot be that anyone who receives a direct signal escapes liability by becoming a party to the communication. Someone who presses up against a door to listen to a conversation is no less an eavesdropper just because the sound waves from the next room reach his ears directly. That person remains a third party, even as a direct recipient of the speaker's communication.

*Revitch v. New Moosejaw, LLC*, No. 18-CV-06827-VC, 2019 WL 5485330, at *2 (N.D. Cal. Oct. 23, 2019); *see also Saleh v. Nike, Inc*., 562 F. Supp. 3d 503, 521 (C.D. Cal. 2021) (finding that software-as-a-service provider did not become a "party" to the communication "simply because it was providing recording and transmission services" for a website).[11] This is consistent with recommendations by the Federal Trade Commission:

---

[10] "The burden of establishing the existence of an agency relationship is on the party asserting it." *Castle Cheese, Inc. v. MS Produce, Inc.*, 2008 WL 4372856, at *6 (W.D. Pa. Sept. 19, 2008) (citing *Goodway Mktg., Inc. v. Faulkner Adver. Ass'n, Inc.*, 545 F. Supp. 263, 267 (E.D. Pa. 1982)).

[11] Notably, the reasoning in Defendants' key citation for the proposition that analytics software and a website should be viewed as "one in the same for purposes of analyzing a wiretapping claim," *Graham v. Noom*, 533 F. Supp. 3d 823 (N.D. Cal. 2021), has already been explicitly rejected *twice* in the Northern District of California alone. *See Cody v. Ring LLC*, No. 23-CV-00562-AMO, 2024 WL 735667, at *6 (N.D. Cal. Feb. 22, 2024) (rejecting *Graham's* interpretation of California privacy statute and finding that "a vendor hired by a website may act

> The Commission maintains the view that [data sharing] affiliates are third parties, and a consumer choice mechanism is necessary unless the affiliate relationship is clear to consumers. Common branding is one way of making the affiliate relationship clear to consumers. By contrast, where an affiliate relationship is hidden—such as between an online publisher that provides content to consumers through its website and an ad network that invisibly tracks consumers' activities on the site—marketing from the affiliate would not be consistent with a transaction on, or the consumer's relationship with, that website. In this scenario consumers should receive a choice about whether to allow the ad network to collect data about their activities on the publisher's site.

FTC Report, Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers (March 2012) (emphasis added).[12]

Defendants attempt to buttress this argument by claiming that NaviStone acted as Harriet Carter's "agent" under Pennsylvania law, but this argument ignores key facts about NaviStone's autonomy and use of the data it collected from Harriet Carter's website visitors. Under Pennsylvania law, "an agent is one who acts in the place and stead of another." *Commonwealth v. Britton*, 229 A.3d 590, 597 (Pa. 2020) (citation omitted). Moreover, an agency relationship only exists where "a principal exerts *actual control* over the work of the agent;" the right to control must be as to the *manner* of the work and not just the end result of the work. *Castle Cheese, Inc.*, 2008 WL 4372856 at *7 (citations omitted). NaviStone did not "act in the place and stead" of its clients, including Harriet Carter.[13] Instead, it deployed its proprietary software on Harriet

---

as a third-party eavesdropper if it secretly records conversations in real time"); *Javier v. Assurance IQ, LLC,* 649 F. Supp. 3d 891, 899–900 (N.D. Cal. 2023) (similar).

[12] https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

[13] Defendants argue that NaviStone's role was simply "akin to that of a third-party call center answering calls placed to a retailer and taking orders on the retailer's behalf." MSJ at 13. But this fundamentally misconstrues the facts. Using the call center analogy, NaviStone's role was actually that of a third-party that a retailer solicited to secretly listen in on calls to its call center, which then used the fruits of that eavesdropping to track down and call the customer back later to sell them products. This role straightforwardly runs afoul of WESCA, which "requires all

Carter's website to intercept visitor data, and it had significant autonomy as to the operation of this software and usage of the data it collected. The user data that NaviStone maintains in its server is all controlled by and accessible to NaviStone. CSOMF ¶ 392. While the OneTag code was running on Harriet Carter's website, NaviStone could have made, and indeed did make, changes to what information the Code collected at any time without notifying Harriet Carter.[14] CSOMF ¶ 389. After NaviStone intercepted users' communications, it further transmitted pseudonymous cookies identifying each user to other third-parties, which in turn ultimately link that cookie to a name and address. CSOMF ¶¶ 393–94, 495. And although NaviStone maintained client-specific cookie identifiers, it also maintained third party cookies that remained the same for each browser across all of NaviStone's clients' websites and Harriet Carter's users' data was not segregated from NaviStone's other clients' user data. CSOMF ¶¶ 5,108. 210. All of these facts demonstrate that Harriet Carter was not directing and controlling the day-to-day actions of NaviStone and no agency relationship existed.

Whether or not NaviStone was acting as Harriet Carter's "agent" should not distract the Court from the central issue in this action on remand: consent. As the Third Circuit emphasized in its prior decision, NaviStone and Harriet Carter cannot avoid liability under WESCA "merely by showing that Plaintiff communicated directly with NaviStone's servers," but must instead establish consent to the interception. *Popa,* 52 F.4th at 128-29. Defendants have failed to do so.

---

parties—not just a party—to consent" to an interception. *Popa*, 52 F.4th at 128, 133 (citing 18 Pa. C.S. § 5704(4)); *see also Commonwealth v. Murray*, 223 A.2d 102, 108 (Pa. 1966).

[14] NaviStone did just that in 2017 when, in response to news articles about its wiretapping, it changed the Code to discontinue searching for and capturing email addresses input into the Harriet Carter website by users. CSOMF ¶ 389.

## II. Visitors to the Harriet Carter Website Did Not Give Implied Consent to the Interception and Transmission of Their Communications.

As set forth above, Plaintiff did not consent to the interception of her communications with the Harriet Carter website simply because either recipient may have been a direct recipient. Defendants' have also failed to prove that Plaintiff gave implied consent to that interception, either.

Plaintiff did not know, nor should have known, that her communications were being surreptitiously intercepted. Plaintiff, like over 99% of visitors to Harriet Carter's website, never saw the Harriet Carter privacy policy—which was insufficient to inform her about NaviStone's data collection practices regardless. And Plaintiff had no idea that third-party code could be deployed on retailer websites to intercept her communications, nor did she have any knowledge of tools that could uncover NaviStone's code.

### A. Harriet Carter's privacy policy—viewed by less than 1% of website visitors—did not create implied consent.

Defendants suggest they cannot be held liable under WESCA because Harriet Carter's privacy policy, or "Privacy Statement," created implied consent on Plaintiff's behalf. While the evidence is uncontroverted that Plaintiff had no subjective knowledge of the interception, even when applying the objective reasonable person standard, Defendants cannot meet their burden to prove consent.

First, Harriet Carter made design choices that led to less than 1% of website visitors ever viewing the Privacy Statement. Second, NaviStone's OneTag deployed and intercepted users' communications before they could even read the Privacy Statement and decide to continue using the website, meaning that no visitor could have given their consent before the interception began. And third, even if a visitor managed to view the privacy policy, the content and design of the

policy prevented a reasonable visitor from meaningfully understanding that NaviStone was intercepting their communications.

*a. Less than 1% of visitors ever found the Harriet Carter privacy policy.*

Preliminarily, it strains logic to suggest that the privacy policy was sufficient to obtain Internet users' prior consent to the interception of their communications by NaviStone when barely any users even saw the privacy policy in the first place. It is undisputed that less than 1% of users to the Harriet Carter website ever navigated to the website's privacy policy while NaviStone's Code was deployed. CSOMF ¶ 436. In line with this trend, Plaintiff herself does not recall ever finding or reading Harriet Carter's privacy policy. CSOMF ¶ 176.

Defendants could have fixed this issue through an array of alternative methods of presenting a privacy policy and their data collection practices. Cookie banners and pop-ups, for example, were always available and also became much more common at the time Defendants' wiretapped Plaintiff. CSOMF ¶ 418. Other strategies also exist to alert users to the collection of their data, such as visceral notices using sound, color, or audio alerts. CSOMF ¶ 420. These pop-up notifications or "just in time" notifications can let individuals know about data extraction at the moment it is about to happen, giving them the opportunity to opt in or opt out and give proper consent. CSOMF ¶ 419. Despite this array of tools, Harriet Carter did not have, and never considered, a pop-up or banner alerting users to its privacy policy during the relevant time period. CSOMF ¶ 432. And Harriet Carter never required website visitors to read or accept its privacy policy when they visited the site. CSOMF ¶ 434.

Defendants also argue that Harriet Carter's placement of a link to their privacy policy was more than sufficient in 2018 because this means of presenting their policy was common practice at the time. But in the context of WESCA, the commonality of a practice does not inherently mean that the practice comports with the law or that a practice constitutes sufficient

prior consent. *See Murray*, 223 A.2d at 108–09. Indeed, Plaintiff's expert Ari Waldman explained that, although placing privacy policy links in a website footer may be common, this practice nonetheless leads to website users completely missing the privacy policy and using a website "without ever seeing, reading, or having to agree to privacy policy terms." CSOMF ¶ 399.

Moreover, Defendants' argument that Plaintiff consented to the information laid out in the Privacy Statement simply by virtue of browsing the website falls flat in light of emerging caselaw rejecting the validity of so-called "browsewrap" agreements. "In browsewrap agreements, a company's terms and conditions are generally posted on a website via hyperlink at the bottom of the screen." *James v. Glob. TelLink Corp*, 852 F.3d 262, 267 (3d Cir. 2017). "Unlike online agreements where users must click on an acceptance after being presented with terms . . . browsewrap agreements do not require users to expressly manifest assent." *Id*. The enforceability of a browsewrap agreement generally turns on whether the terms or a hyperlink to the terms are reasonably conspicuous on a webpage. *Id*. When terms are linked at the bottom of a webpage where users are unlikely to see it, courts have refused to find constructive notice. *See id.* (citing *Nicosia v. Amazon.com, Inc.*, 834 F.3d 220, 233 (2d Cir. 2016)). However, where the website has an "explicit textual notice that continued use will act as a manifestation of the user's intent to be bound," courts are more willing to assume a user's consent to terms contained in the linked webpage. *Id.* (citing *Nguyen v. Barnes & Noble Inc*., 763 F.3d 1171, 1177 (9th Cir. 2014)).

Though browsewrap enforceability most frequently arises in the context of a website's terms and conditions, courts have also applied these principles to determine whether website users had constructive notice of a website's privacy policy. *See, e.g., Yoon v. Lululemon USA, Inc*., 549 F. Supp. 3d 1073, 1081 (C.D. Cal. 2021) (citing *Nguyen*, 763 F.3d at 1178–79, and finding that user did not consent to privacy policy where policy did not provide sufficient notice

to users or prompt them to take any affirmative action to demonstrate assent). Here, there is no evidence that Harriet Carter ever required users to affirmatively consent to the privacy policy or otherwise included language that continued use of the website would act as a manifestation of a user's consent to the Privacy Statement. As such, the Privacy Statement is an unenforceable browsewrap agreement.

Harriet Carter's use of a link on the footer of its website to alert users to its privacy policy was insufficient to obtain users' implied consent to NaviStone's interception of their communications, particularly given that one of Defendants' own experts testified that it would have been "technologically possible *since day one*" to provide privacy disclosures in ways other than a hyperlink to a static privacy document. CSOMF ¶ 433 (emphasis added).

*b. NaviStone's code intercepted communications immediately, even if all a visitor did was navigate to the Harriet Carter privacy policy, making prior consent impossible.*

Implied consent also cannot be inferred from the existence of the Harriet Carter Privacy Statement because NaviStone's OneTag deployed and intercepted users' communications *before* they could even read the Privacy Statement.

Under WESCA's all-party consent exception, an entity does not violate WESCA if the entity intercepts communications where "all parties to the communication have given *prior consent* to such interception." *Popa*, 52 F.4th at 128 (citing 18 Pa. C.S. § 5704(4)). Here, NaviStone's OneTag began intercepting a website visitor's communications immediately upon their arrival to any page of the Harriet Carter website, making it impossible for Defendants to obtain users' "prior" consent by function of the Privacy Statement. CSOMF ¶ 384. OneTag deployed at the time of the page loaded, and the likelihood that any visitor could click on the link to the Privacy Statement—let alone read and understand the lengthy Privacy Statement—before OneTag intercepted their communications is extremely low. CSOMF ¶¶ 385–386.

As conceded by Defendants' own expert, even if someone visited the Harriet Carter website specifically to view the privacy policy, OneTag was configured to operate on the Harriet Carter Privacy Statement itself, and navigation to the policy would result in the deployment of OneTag's Code and the transmission of a payload of information to NaviStone that included, at minimum, a user's IP address, the specific page title (in this example, Privacy Statement), and a detailed URL showing that the user requested to view the Privacy Statement. CSOMF ¶ 485. Contrary to Defendants' assertions, this information *is* descriptive content regarding a user's website visit. Indeed, the Third Circuit has already highlighted that one of the key pieces of "communications" that NaviStone captured from Plaintiff was "which pages she visited." *See Popa*, 52 F.4th at 124.

Defendants claim that there was no interception for visitors who only viewed the Privacy Statement page, because OneTag did not collect sufficiently personal information from these visitors. But this improperly reframes the proper inquiry under WESCA, and the proper inquiry in this case on remand. WESCA defines "contents" broadly as "*any* information concerning the substance, purport, or meaning of that communication," 18 Pa. C.S. § 5702 (emphasis added), and the proper question under WESCA is not *what* content was intercepted, but *whether* content was intercepted. *See Popa*, 52 F. 4th at 129 (quoting *Commonwealth v. Shreffler*, 201 A.3d 757, 764 (Pa. Super. Ct. 2018)) (noting that WESCA "is to be strictly construed to protect individual privacy rights"). For the common law privacy torts that legislatures codified and expanded through wiretapping statutes like WESCA, the violation of someone's privacy turned on the *act* of intrusion or interception, not whether the intruder acquired any sensitive information through the intrusion. *See* Restatement (Second) of Torts, § 652B; *see also In re Marriage of Tigges*, 758 N.W.2d 824, 830 (Iowa 2008) (holding tortfeasor's liability arose from his recording his wife's

activities without her knowledge or consent, not from the specific nature of the recorded activities). Moreover, many courts have already recognized that the information collected when a user visited just the Harriet Carter Privacy Statement is sufficiently substantive to be considered "contents" under WESCA. *See In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 139 n.50 (3d Cir. 2015) (query URLs and URLs , if detailed, may be content); *see also In re U.S. for an Order Authorizing the Use of a Pen Register & Trap*, 396 F. Supp. 2d 45, 50 (D. Mass. 2005) ("contents" includes URL "subject lines, application commands, search queries, requested file names, and file paths."). This Court should do the same.

Ultimately, however, this disagreement over the significance of the intercepted information should not distract from the key fact here: NaviStone intercepted the communications of Plaintiff and other website visitors well before they could find or review the Privacy Statement. The Privacy Statement, therefore, cannot be used to imply users' *prior* consent to this interception.

*c. The content of the Privacy Statement was insufficient to provide the average website visitor notice of the interception, such that they could have given their consent to the interception of their communications.*

If the Court finds that the Privacy Statement could serve as a basis for implied consent—even though it was structured as a browsewrap policy, was never viewed by most website visitors, and OneTag would deploy well before any visitor could actually read the policy—the content of the Privacy Statement is insufficient to garner users' consent to NaviStone's practices.

First, the Privacy Statement uses deceptive framing in order to deceive visitors into thinking that Harriet Carter will protect their privacy and not collect their data without their consent. The policy's very first paragraph stated that Harriet Carter "believe[s] you have a right to a safe, secure online shopping experience. We are committed to both protecting your privacy." CSOMF ¶ 438. Similarly, later provisions in the Privacy Statement profess that Harriet Carter

"adopts an 'opt-in' mentality to all promotional information," including customer lists, promotional emails, and catalog mailings. CSOMF ¶ 439. Despite these express statements about privacy and Harriet Carter's alleged opt-in approach, NaviStone's OneTag collected users' data regardless of whether they "opted-in" and consented to receiving promotional materials.

Second, the Privacy Statement buries information about NaviStone's interceptions deep within the policy and beneath an illogical heading. There is no information about NaviStone's wiretap in the first section of the policy, where someone would logically look to determine "what information is gathered" from visitors (because the heading says just that). CSOMF ¶ 441. Instead, the paragraph Defendants claim alludes to NaviStone's activity is under the "Who Else Has Access to the Information I Provide to HarrietCarter.com?" section, tucked away under a sub-section titled "Third Party." CSOMF ¶ 442. But even this section is not straightforward, beginning with a discussion about visitors who buy gifts for their friends, and a promise that "HarrietCarter.com does not sell, rent, or give away your personal information to anyone." CSOMF ¶ 443. Only at the very bottom of this section does the policy suggest, contrary to its express opt-in statement, that Harriet Carter "may from time to time contract with third party vendors to serve ads . . . or to send our catalogs to customers." CSOMF ¶ 444. Objectively, the average visitor would struggle to find this statement, even if they were looking for information on data tracking and collection that was occurring on the Harriet Carter website.

Third, this generic reference to online ads and catalog mailings does not provide a clear or accurate explanation of who the vendors are, how they are getting the user's data, or what that data consists of. CSOMF ¶ 446. There is no mention of NaviStone's name anywhere in the policy. CSOMF ¶ 446. The Privacy Statement erroneously claims that any third-party vendors operating on the website will only collect "anonymous information" about website visitors, even

though NaviStone's OneTag collects pseudonymous information that can be used to deanonymize visitors and uncover their name and mailing address. CSOMF ¶¶ 384–85, 442. And the Privacy Policy's statement that information is collected through use of a "cookie or pixel tag" is incomplete and misleading, as NaviStone's OneTag captures users' communications through a proprietary Javascript code, which will still deploy even if a user disables cookies. CSOMF ¶ 441. Put simply, the Privacy Statement does not adequately inform users of Defendants' conduct in order to obtain consent. CSOMF ¶¶ 436–441. Defendants' own expert agrees that, if NaviStone's OneTag is capturing users' communications, the privacy policy does not reflect how that interception is occurring. CSOMF ¶¶ 441, 469.

Taken together, these facts demonstrate that the contents of Harriet Carter's privacy policy were insufficient to solicit users' consent to NaviStone's interception of their communications, which occurred from the moment that visitors arrived on the Harriet Carter website.

**B. The use of third-party code elsewhere on the Internet does not create implied consent to Defendants' interception of web visitors' communications in this case.**

Defendants also assert that Plaintiff consented to the interception of her communications simply because third-party code like NaviStone's OneTag is ubiquitous on the Internet, and website visitors like Plaintiff should have known that such code was being deployed simply by being online. This argument is unavailing, as a device's widespread use does not excuse the need to seek consent before deploying it under WESCA—and as demonstrated by Ms. Popa's testimony, widespread use does not inherently beget widespread *knowledge* of the device's existence or capabilities.

Over half a century ago, the Pennsylvania Supreme Court firmly rejected the notion that the universality of an intercepting device can somehow excuse the need to seek consent before

that device is used to intercept communications. In a case applying WESCA to the use of a telephone extension to listen in on an individual's conversation, the state's highest court explained:

> All the prattle about the universality of the telephone extension is utterly irrelevant to this case. The lower Court said:
>
> 'It is commonplace for the ordinary home owner to have several telephone extensions in his home, e.g., one in the hall, another in the bedroom, a third in the kitchen, and a fourth in his office or den.'
>
> It is not known in what affluent neighborhood the lower Court lives that the homes of all its friends are equipped with a vast, multiple-telephone system more appropriate to a fire engine station than to the 'ordinary' private dwelling. The 'ordinary' homeowners that the writer of this Opinion visits usually have one telephone in the hall or the living room, and that is it.
>
> However, even assuming that the home of the Trial Judge has ten telephone extensions, is this an invitation for ten neighbors to come in and eavesdrop on his private conversations? **And then, the commonplaceness of any device or object is not the criterion for determining the innocence or criminality of its employment.** No object can be more commonplace than a kitchen knife, but when it is used to stab someone to death, the ordinariness of the knife does not render it any less a homicidal weapon. It is not what the telephone extension Is that may make it illegal in certain circumstances, but the Use to which it is put.

*Commonwealth v. Murray*, 223 A.2d 102, 108–09 (Pa. 1966) (emphasis added). Likewise here, third-party software might be deployed in ways that do not run afoul of the law, including WESCA. But where third-party software is used to eavesdrop on website visitors' communications without their consent, the ubiquity of that software is not an excuse to claim that the visitors impliedly consented to the software's surreptitious collection of their information.

Plaintiff's own experience demonstrates that common use of third-party code does not inherently indicate that deployment of such code is common knowledge among website visitors. When she visited Harriet Carter's website, Plaintiff had no idea that NaviStone's OneTag was operating on the web page and was actively intercepting her private information. CSOMF ¶ 466. Upon discovering the possibility that her communications Harriet Carter's might have been

intercepted, she immediately asked her attorney about her legal rights because she found such a practice "very disturbing." CSOMF ¶ 467. Indeed, prior to her first deposition in this case, Ms. Popa was not aware that retailer websites might have other third-party content on their website, such as images. CSOMF ¶ 465. Similarly, despite their widespread use, Plaintiff is unaware of other third-party analytics tools like Google Analytics, or online advertising networks more generally. CSOMF ¶ 472. This lack of awareness is not limited to Plaintiff. One study of individuals' knowledge about data tracking online found that over eighty percent of the individuals involved earned failing or close-to-failing grades when asked to answer questions about online data collection practices. CSOMF ¶ 413. Conversely, Plaintiff's technical expert Jason Frankovitz testified that he is only aware that he is interacting with pieces of software of unknown origin when he visits a website because he has been "working with the web since the mid-90s" and is "a little bit more of a sophisticated user than regular noncomputer science type of people." CSOMF ¶ 414. Despite Defendants' assertions that the use of third-party code like NaviStone's is widespread and well-known, Plaintiff's own testimony—and that of her expert—demonstrates that the use of this code is not nearly as well-known as Defendants suggest.[15]

Even with Plaintiff's newfound awareness that third-party code can secretly intercept her communications online, she—like many less technology-literate web users—has no knowledge of how to even discover if such code is running, or the power to stop it from deploying. Defendants claim that use of such technology is no secret and assert that various resources exist

[15] Defendants also suggest that Plaintiff should have known that Harriet Carter was allowing third parties to intercept her communications given her previous role as a contract nurse for Cigna. This comparison between Plaintiff's employment as a nurse and the surreptitious deployment of NaviStone's code on the Harriet Carter website compares apples to oranges. Indeed, Plaintiff herself testified in her deposition that such a comparison was "very hypothetical," and she wasn't sure how to respond to such a question. CSOMF ¶ 468.

to see what third-party tools are running on a given website, including a website called BuiltWith. But much like third-party code, the existence of these resources is not well-known.[16] Plaintiff, for example, testified at her deposition that she "wouldn't even know how to" determine if NaviStone's code was running on websites that she visits. CSOMF ¶ 471.

These tools are also insufficient to adequately inform users about the full extent of any interception by third-party code. Using these strategies, for example, will not necessarily reveal the full extent of what data a third-party like NaviStone is collecting or what it is capable of doing with that data. As Defendants' own expert testified, although tools like BuiltWith can reveal what third-party code is running on a given website, those tools will not demonstrate every website or company that is part of the data sharing networks of the companies deploying that code. CSOMF ¶ 494-95.[17] Moreover, while Defendants assert that individuals can deploy an array of tools to prevent tracking and interception software, such as "denying" cookies or installing an ad blocker, many of these tools would not stop NaviStone's Javascript code from functioning. CSOMF ¶ 247; *see also* CSOMF ¶ 61 (ad-blocking software would only block OneTag from running if user was aware that separate domain under different name, not NaviStone.com, would need to be blocked); CSOMF ¶ 63 (disabling first-party cookies and third-party cookies will not prevent NaviStone's data collection); CSOMF ¶ 103 (users on "do-not-mail" lists still have their data collected by NaviStone).

[16] Nor should a user have to navigate to an entirely separate website and investigate what Harriet Carter is doing with their communications. Requiring a user to conduct a separate investigation on a different site for every web page they visit logically cannot constitute consent.

[17] In the case of NaviStone, a visitor to the Harriet Carter website would not be able to uncover that NaviStone subsequently sends their data to Neustar, which NaviStone uses to connect the PII it intercepts with website visitors' names and mailing addresses. CSOMF ¶ 365. Nor would users like Plaintiff be able to view every website or every company that is a part of the Neustar data sharing network. *Id.*

In sum, Defendants' suggestion that Internet users consent to the interception of their communications by the nature of the internet ignores key facts in evidence, which create critical and genuine factual disputes about what users like Plaintiff know or should have known. To find that Plaintiff consented to the interception by the nature of the internet also goes against Pennsylvania law, which holds that the commonality of a device does not excuse the need to seek consent before using it for an interception under WESCA. *Murray*, 223 A.2d 102, 108–09 (Pa. 1966). Indeed, accepting Defendants' position that Plaintiff and others consented to the surreptitious interception of their online communications merely by being active users of the Internet would essentially render WESCA, as it applies to electronic communications, wholly meaningless. *See* 1 Pa. C.S.A. § 1922 (the ***entire statute*** is intended to be effective and certain).

## III. Applying the plain meaning of WESCA in these circumstances comports with Pennsylvania rules of statutory construction and constitutional principles.

Since the start of this case, Defendants have engaged in endless fearmongering over potential societal outcomes that might occur if the Court finds them liable for wiretapping Plaintiff's communications. This Court and the Third Circuit have rejected Defendants' "Hail Mary" constitutional and societal arguments before, and the Court should reject such arguments again here.

First, "everyone is doing it" is no defense to liability under WESCA. *See Murray*, 223 A.2d at 109 (emphasizing that "the commonplaceness of any device or object is not the criterion for determining the innocence or criminality of its employment" for purposes of WESCA). The notion that this Court should rule in Defendants' favor simply because doing so will alter the way that many technology companies conduct their business is unavailing. Rather than being an "absurd" ruling that criminalizes the Internet, an adverse ruling for Defendants would result in a simple and straightforward outcome for the Internet more broadly: companies like HCG (who

procured NaviStone to intercept communications) and NaviStone (who intercept those communications) would have to be more transparent about their data collection conduct, in order to properly obtain web users' consent for any interceptions that they engage in. Indeed, privacy laws have been an impetus for such change. Domestic companies doing business in the European Union had to adjust to the strict transparency and consent requirements of the General Data Protection Regulation. Companies doing business in California must comply with the California Consumers Protection Act, which requires, *inter alia*, websites to include a "Do Not Sell My Personal Data" link on their home pages. And although these laws are newer, courts routinely apply existing privacy laws to novel factual scenarios. *See Commonwealth v. Henlen*, 564 A.2d 905, 905 (Pa. 1989) (applying WESCA to what the court considered "novel" factual circumstances); *see also Dittman v. UPMC*, 196 A.3d 1036, 1046 (Pa. 2018).

Defendants' related argument that applying WESCA here would run afoul of the First and Fourteenth Amendment is similarly unconvincing. The Third Circuit itself has already articulated in its prior decision in this case that "[did] not have grave doubts as to the constitutionality of the WESCA." *Popa*, 52 F.4th at 131 n.9. Moreover, many of Defendants' arguments as to the constitutionality of WESCA are rooted in constitutional principles applicable in wholly different contexts. The void-for-vagueness doctrine invoked by Defendants, for example, exists to prevent the imposition of criminal penalties, including incarceration, based on a law that is so vague that an ordinary person could not understand that their conduct was prohibited. *See Kolender v. Lawson*, 461 U.S. 352, 357 (1983); *Jordan v. De George*, 341 U.S. 223, 230 (1951). But in civil cases, the Supreme Court has emphasized that there is "greater tolerance" for vague statutory provisions because "the consequences of imprecision [i.e. civil damages] are qualitatively less severe." *Vill. of Hoffman Ests. v. Flipside, Hoffman Ests., Inc.*, 455 U.S. 489, 498–99 (1982).

Civil business defendants like Harriet Carter and NaviStone also have less entitlement to these types of constitutional canons "because businesses, which face economic demands to plan behavior carefully, can be expected to consult relevant legislation in advance of action." *Id.* Here, though WESCA is technically a criminal statute, Plaintiff here is seeking to enforce the *civil liability* provisions of the statute against two corporations, and Defendants' due process arguments should not concern the Court.[18]

Defendants' constitutional arguments are misdirected and blow the consequences of this case out of proportion. Plaintiff simply seeks to hold Defendants civilly liable for NaviStone's unlawful interception of her communications without her consent. The Third Circuit has already recognized that based on "WESCA's plain language and statutory history," Defendants' actions have been unlawful since at least 2012. *Popa*, 52 F.4th at 129. In this context, the constitutional principles that Defendants invoke are inapplicable, and the Court should reject Defendants' arguments wholesale.

## CONCLUSION

For the reasons discussed above, Plaintiff Popa respectfully requests that the Court deny Defendants' Second Motion for Summary Judgment in its entirety and allow her WESCA claim to proceed to trial.

[18] Similarly, many of the First Amendment cases cited by Defendants involve restrictions on speech in the political and public office contexts—very different circumstances from an attempt to hold corporations liable for tortious conduct. *See, e.g.*, *Citizens United v. FEC*, 558 U.S. 310 (2010) (nonprofit corporation sought to prevent enforcement of civil and criminal penalties for supporting presidential candidate); *Ariz. Free Enter. Club's Freedom Club PAC v. Bennett*, 564 U.S. 721 (2011) (political action committee sought to enjoin state statute limiting campaign financing); *see also People v. Clark,* 6 N.E.3d 154 (Ill. 2014) (holding that state wiretapping statute implicated First Amendment and Due Process concerns in the context of individual criminal prosecution).

Dated: August 15, 2024

Respectfully submitted,

*/s/ Kelly K. Iverson*
Gary F. Lynch (PA 56887)
Kelly K. Iverson (PA 307175)
Jamisen A. Etzel (PA 311554)
Nicholas A. Colella (PA 332699)
Connor P. Hayes (PA 330447)
**LYNCH CARPENTER, LLP**
1133 Penn Avenue, 5th Floor
Pittsburgh, Pennsylvania 15222
Telephone: 412-322-9243
Facsimile: 412-231-0246
gary@lcllp.com
kelly@lcllp.com
jamisen@lcllp.com
nickc@lcllp.com
connorh@lcllp.com

*Counsel for Plaintiff Ashley Popa*